# Application Detection System

**Vamsi Krishna Pelluru**

***Abstract— Across the Globe companies are finding ways to maximize their productivity with infrastructure and Resources, Application Detection system helps companies achieve it, it also helps administrators in identifying which are the applications that are more commonly used across the corporate, those applications can be blocked to use from the networks, Most of the employees spent considerable time in office on Browsing Social Networking sites eg; Face Book, Orkut, LinkedIn etc, Application Detection system helps administrators in identifying the Source machines from which these requests arise, it generates the logs with the source machine IP, Application name , its pattern etc, based on the pattern the corresponding signature will be triggered and it will either block or allow the application based on the configuration provided to it.***

***Index Terms— Application detection System, Signatures.***

## I. INTRODUCTION

This paper presents in detail how a software product that needs to access, interact with, or report applications requires a method of 1) discovering and 2) recognizing those applications. Without strong applications discovery and recognition capabilities data cannot be properly rationalized in an accurate, unified, or truly meaning full manner. Ascertaining which applications are more commonly used in the corporate network is a fairly straightforward process from a technology standpoint. However, there exists no common, standardized method for correlating "discoverable" application data and indicating that to the administrator in a meaningful way.

## II. APPLICATIONS THAT ARE DETECTED BY APP DETECTION SYSTEM

Application Detection System identifies a wide variety of applications traversing through your network, including various voice, streaming audio-video, web-based applications and client and server applications, Games, P2P and business applications

Software package forms a fundamental building block of any state-of-the-art traffic policy enforcement device such as WAF, NAC, next-generation firewall and enterprise WLAN AP. App Detection system is built on top of the platform services package —the middleware framework—which facilitates the migration of networking applications from kernel space to user space without drastically affecting the performance. In general optimizing internet bandwidth is a huge challenge for Corporations. When personals are recruited, corporate have to invest heavily to train these resources and once they are done with training, corporates deploy them on assignments with an expectation that they will get maximum productivity out of them.

**Manuscript received April 2014.**

**Vamsi Krishna Pelluru**, System Validationteam, Freescale Semiconductor, Hyderabad, India.

But does this happen is a million dollar question, the appropriate answer would be "no", they are not used to 100% of their capacity, there can be multiple reasons, generally resources , sometimes the most seasoned campaigners spend most of their times on internet, browsing general websites, and with the recent trend social networking has become a huge hit across the world and most of them stay connected right through the day, which affects work, so

***" How do corporations get out of this? "***

IT Administrators have to analyze the data that flows through their networks, with the current technologies/Tools the generated report may not be of much use. They need a mechanism where they have data from every machine that is there on the network, if such sorts of cutting edge technologies are built, administrators can get data which will suffice their needs.

Data like which machine in the network is using the highest bandwidth, what are the machines that access the most social networking sites, which machines are connected to social networking site for long times, which machines are using the corporate bandwidth to download unwarranted stuff, all these data will allow the admin to either allow or block the traffic based on the corporations IT Policies.

Now comes how the admin will be enabled to do this. In the current scenario developing something like an Application detection software would be apt, what should the software do??, Application Detection Software should be capable of doing the following things:

- ✓ It should detect any packet that enters the network
- ✓ It should read the payload, Notify what content flows in the packet and should also identify the application.
- ✓ Should either allow/block the traffic based on the Corporations IT Policies.
- ✓ It should notify the admin by a mechanism, it can be by logs, which can be logged in to log viewer
- ✓ Notify the Source IP address of the packet, which will help the admin to make an assessment if those particular machines are connected to unwanted sites for long time

These Basic features should be present in any Application Detection software if it has to be of any use to the admin/corporate. Considering the above features the following questions

## III. HOW THIS TECHNOLOGY HAS TO EVOLVE?

What is the Basic frame work one should follow to make this cutting edge technology worthwhile for corporations when they put this for use? The technology has to use "signatures/rules" related to pattern-matching to detect "which application content is flowing in the data flows within the network. Once this is done and a log is generated, it should generally contain the following information: unique ID for the alert, participating agency, indicator/action pair that produced the alert, data and timestamp of the alert, net



*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication Pvt. Ltd.*

flow record, and if applicable, identification of quarantined or captured/stored data associated with the alert.

Signatures/rules can be divided into four logical sections

- Local Section
- Selector Section
- Detect Section
- Action Section

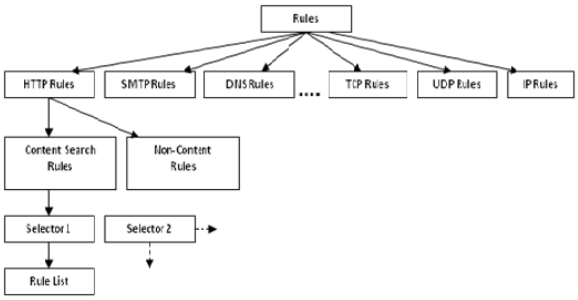
**Local Section** – Local section specifies Rule ID, Log generation attributes, etc, which are management specific information.

**Selector Section** – Selector information contains 5-tuple information.

- Source IP address,
- Destination IP address
- IP protocol information
- Source port and
- Destination port
- Detect Section – Detect Section contains Information on which part of the packet to be inspected, and the pattern that need to be searched.
- Action Section – Action information contains the preventive action that need to be taken upon matching the signature.

Signatures can be classified into various buckets to minimize search space.

- Rules are classified based on Application type, this can be further divided into Content-Search rules, Non-content rules.. (Rules with header fields, flags, integers, etc)




## IV.HOW DOES APP DETECTION SYSTEM WORK

Let's understand how Application detection system primarily performs its operation, by searching for application-specific signatures in the packet data stream, also known as deep packet inspection (DPI). The signatures are loaded on the device at the boot time and get updated periodically. The DPI capabilities of Application detection system allow detection of the supported applications even if they run on non-standard transport ports. This signature-based detection approach is supplemented by protocol analytics, wherever necessary, in order to maximize the accuracy of the results.

## V.HOW SHOULD A SIGNATURE SEARCH HAPPEN?

- ✓ Detection engine should invoke matched application engine to get its accumulated buffers (Extracted data during pre-processing) for signature searching.
- ✓ Applications should provide multiple buffers and their pattern types for searching. (For example, HTTP Engine can provide URI buffer, MIME buffer, HTTP_RAW buffer at a time).
- ✓ Software DFA, PCRE, and Hardware DFA combinations are used for pattern matching.
- ✓ Detection core goes through relevant Rules (signatures) for matching these buffers. (All URI based signatures are searched on URI buffer).
- ✓ If available, Hardware DFA will be invoked with right search tree IDs.

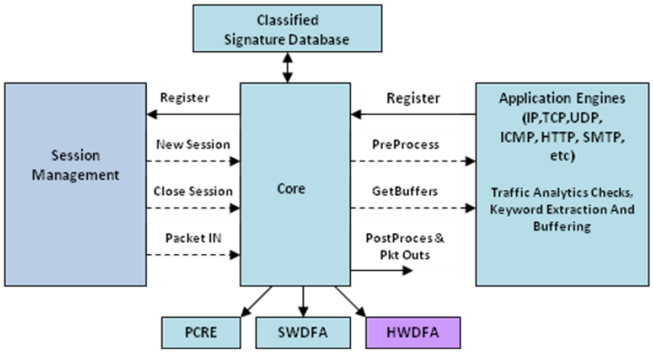
## VI. APPLICATION DETECTION SYSTEM PRE-PROCESSING

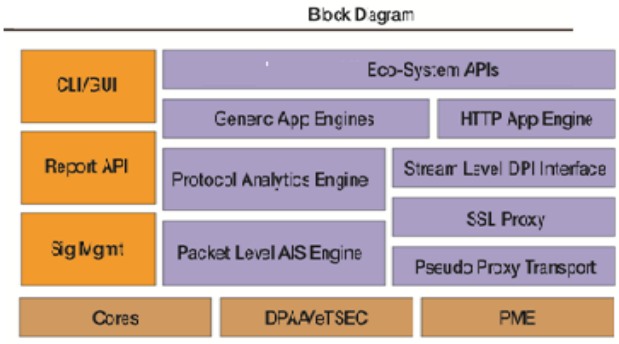
- ✓ Sessions are classified across IP, Transport and Application protocols (HTTP, SMTP etc).
- ✓ Pre-Processing decodes each packet, and invokes matched application engine for further processing.
- ✓ Each application engine parses the packet to extract Keyword specific data from the packet. (For example, HTTP engine extracts URI, MIME fields from HTTP packet)

## VII. POST PROCESSING

- ✓ Application detection software Post processing verifies Signature/rules search results for completeness of rule.
- ✓ Non-Content signatures are verified as part of post processing
- ✓ ADS will notify the registered policy enforcement software packages, such as WAF or QoS..

## VII. HOW WILL GENERAL APPLICATION IDENTIFICATION SOFTWARE STACK LOOK LIKE?




## VIII. EVOLUTION OF TRAFFIC ANALYSIS

The principal catalyst for deploying DPI has been the rapid migration of network traffic to IP, and the related explosion in the use of applications and content delivered "over the top" to a widening range of devices, including smart phones and tablet computers. This has created new challenges for operators in managing traffic and customer quality of experience (QoE); understanding the nature of IP packet flows has become critically important to providing an acceptable level of service at an acceptable cost.



*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication Pvt. Ltd.*

## IX. POTENTIAL CUSTOMERS/USERS OF APPLICATION DETECTION SYSTEM

1. Service assurance (QoS, QoE)
2. Policy Control (PCEF)
3. Gateways
4. Service Routers
5. Load balancers
6. Congestion control

## VIII. CONCLUSION

Two thirds of Corporates now believe Application detection System is a must-have technology, the largest use case is service assurance for QoS/QoE; the second largest is policy control (PCEF), which will be the largest use case by volume, The proportion of corporates choosing to source DPI from a third party is gradually rising, and a majority of those doing so prefer to use a pure-play supplier of DPI components. Encryption of protocols is reducing the effectiveness of DPI. Packet metric analysis (heuristics) was identified as the main remedy.

## ACKNOWLEDGMENT

Would like to thank MR T.V.Rao for introducing me to this technology.

## REFERENCES

[1] http://www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html
[2] http://www.deeppacketinspection.ca/

Vamsi Krishna Pelluru Completed Masters in Computer Applications from Kakatiya University, working as Senior Quality Assurance Engineer in Freescale Semiconductor for the past Eight years, his expertise lies across network security, Open Stack and Storage Area Networks.



*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication Pvt. Ltd.*